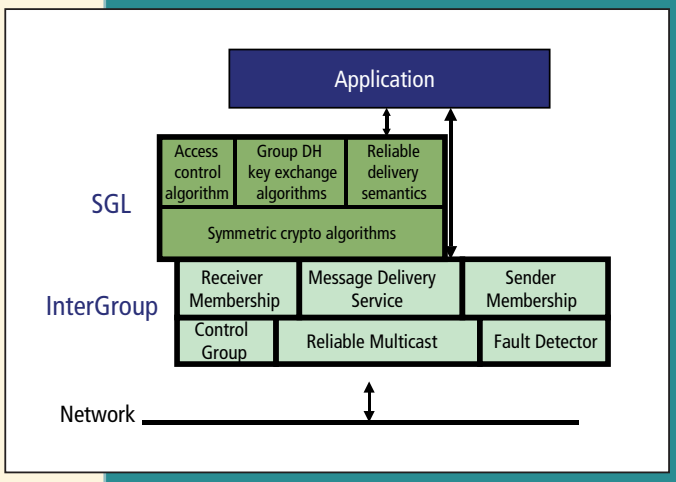
Enabling Ad-hoc Secure Peer-to-Peer Collaboration

Current collaboration tools and environments, such as the Access Grid (AG) and the Pervasive Collaborative Computing Environment (PCCE), provide a set of persistent services to users. However, they often rely on a centralized infrastructure. For example, a user wishing to join an AG or PCCE venue must connect to a server. This makes the tools impossible to use when a specific resource or server is unavailable. Ideally, the collaboration environment should not depend on any specific resource or server; instead, the resources and servers should add value to the system when they are present. In addition, this infrastructure-centric approach makes these tools difficult to set up and scale, particularly when security is involved. A collaboration environment should be structured to support informal, spontaneous collaborations as well as highly structured environments. Using on-line tools, it should be easy to begin collaborating, and incrementally add users and services as needed.

At its core, a collaboration environment depends on the users being able to reliably communicate with each other and knowing the identities of the other collaborators. When the session is conducted over an untrusted network, such as the Internet, it is essential to provide security. This allows the legitimate collaborators to feel confident about the identities of their partners and securely communicate with them. Although it is possible to establish communication among the collaborators using unicast mechanisms (TCP and SSL), this is very complex, inefficient, and hard to scale. Instead, a natural underlying communication layer for a collaboration environment is secure, reliable multicast.

An ideal instantiation of secure, reliable multicast communication is provided by a combination of the InterGroup protocols and the Secure Group Layer (SGL). The InterGroup protocols are reliable multicast protocols that scale to the Internet and provide membership services, reli-



Typically, reliable ordered group communication protocols have been developed for local-area networks, and do not, in general, scale well to large numbers of nodes and wide-area networks. The InterGroup suite of protocols is intended for a wide-area network with many nodes, highly variable delays, and message loss, such as the Internet. It uses an unusual approach to group membership and message delivery. The group membership is in fact two memberships. The first membership is all participants in the group and the second membership is the currently active senders. This second membership makes tracking of outstanding messages easier and improves scaling. The protocols allow messages to be delivered with different levels of ordering and reliability. Each receiver makes the choice of which service level to use. The levels of message delivery service range from unreliable/unordered to reliable/timestamp-ordered.

The challenge with security services for group communication is how to best provide them to the application. Securing these messages requires a layer similar to Secure Sockets Layer (SSL), but designed for multicast. We have designed such a layer protocol called Secure Group Layer (SGL) that provides a security context within which messages multicast over the wire can be cryptographically protected. The essential building block for setting up a secure multicast context is a key exchange protocol that allows the participants to exchange a session key as peers. An important step in solving this problem is to design algorithms that allow a set of participants to agree on a session key. We have designed group Diffie-Hellman key exchange algorithms to solve this problem. We are also working on mechanisms to enforce restrictions on who can participate in the key exchange. SGL is a security layer that merges the Diffie-Hellman key exchange and the access control mechanisms.

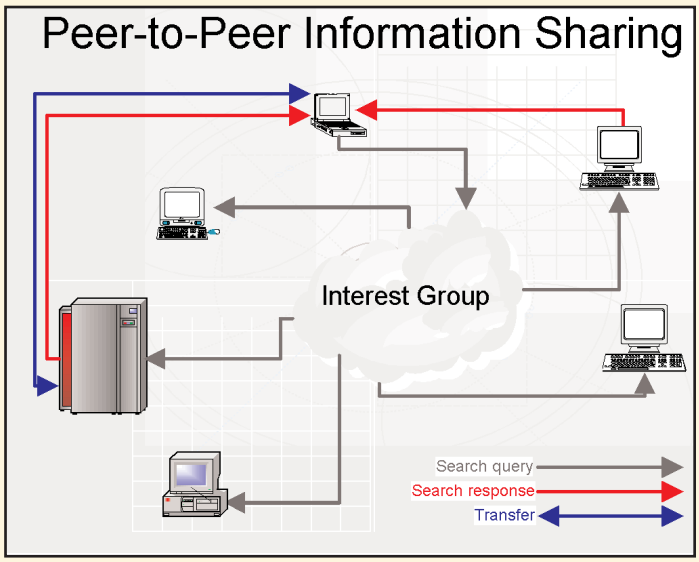
SciDAC
Scientific Discovery through Advanced Computing

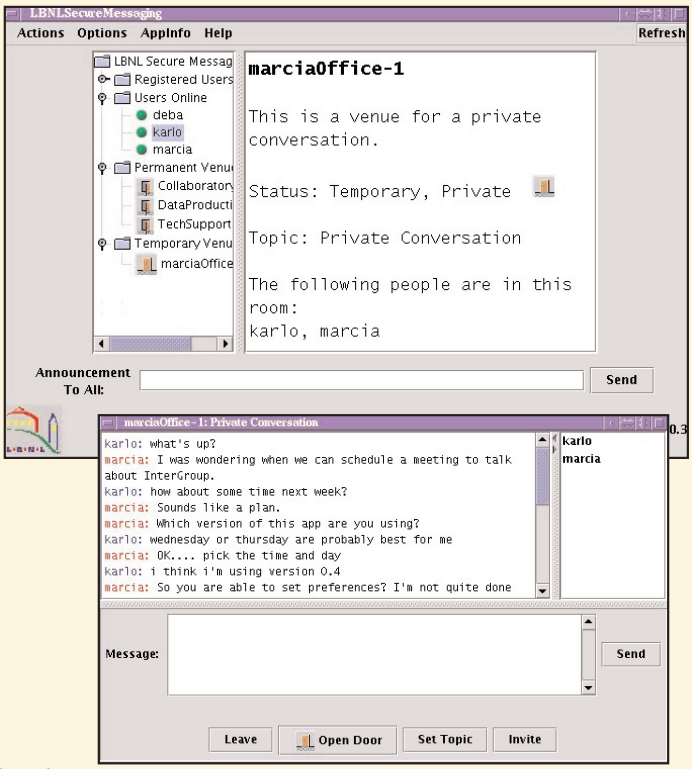
able message delivery, and ordered message delivery. The Secure Group Layer (SGL) provides the security services required by applications utilizing reliable group communication in wide-area environments. SGL establishes secure multicast channels among application components. A secure multicast channel is built by establishing a session key among the legitimate application components. This key is then used to achieve multicast message confidentiality and/or multicast data integrity.

An example of a collaborative application based on InterGroup and SGL is the information-sharing and discovery system we are currently developing. It will enable scientists to store and manage information on local storage facilities while sharing them with remote participants. This system is designed, from the ground up, as a collaboration tool built upon the principal of ad-hoc, secure collaboration. The core components of this system will be reused to further enable this type of collaboration within other tools and environments such as the PCCE.

The PCCE system currently relies on a server to coordinate collaborator activities. This server keeps track of the set of authorized users, the set of users currently participating in the collaboration, and the tools available in the environment. This design forces users of PCCE to rely on this server. PCCE is migrating to using an InterGroup and SGL core for communication so that the collaboration can operate without the PCCE server. By removing the dependence on the server, PCCE gains the ability to run in a purely ad-hoc manner. The PCCE server, if present, will enhance the functionality of the collaboration.

By using InterGroup and SGL as core communication services in the collaboration environment, existing collaborations can easily operate in either an ad hoc or infrastructure-enabled setting. This allows servers to provide added value services rather than being essential components. Thus, the dependence on centralized infrastructure is reduced and informal, spontaneous collaborations are enabled.





FUNDING: This research is funded by the U.S. Department of Energy, Office of Science's Office of Advanced Scientific Computing Research, Mathematical, Information and Computational Sciences Division.

FOR MORE INFORMATION ABOUT THIS WORK, GO TO
http://www-itg.lbl.gov/Collaboratories/